

(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11) 特許出願公表番号  
特表2003-504723  
(P2003-504723A)

(43) 公表日 平成15年2月4日(2003.2.4)

(51) Int.Cl.<sup>7</sup>  
G 0 6 F 13/00

識別記号  
3 5 1

F I  
G 0 6 F 13/00

テーマコード(参考)  
3 5 1 Z 5 B 0 8 9

審査請求 未請求 予備審査請求 有 (全 33 頁)

(21) 出願番号 特願2001-508692(P2001-508692)  
(86) (22) 出願日 平成12年6月29日(2000.6.29)  
(85) 翻訳文提出日 平成14年1月4日(2002.1.4)  
(86) 国際出願番号 P C T / I L 0 0 / 0 0 3 7 8  
(87) 国際公開番号 W O 0 1 / 0 0 2 9 6 3  
(87) 国際公開日 平成13年1月11日(2001.1.11)  
(31) 優先権主張番号 0 9 / 3 4 5 , 9 2 0  
(32) 優先日 平成11年7月1日(1999.7.1)  
(33) 優先権主張国 米国 (U S)

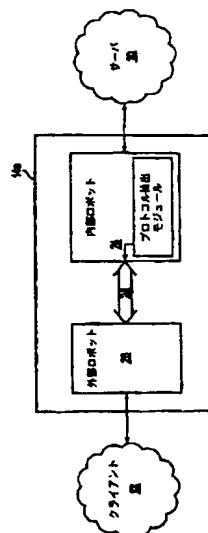
(71) 出願人 サンクタム、リミテッド  
イスラエル国、ヘルズリヤ、サビア ストリート 1、ビー、オー、ボックス 12047  
(72) 発明者 ラーナン、ギル  
イスラエル国 ゾラン、ハダリム ストリート 19  
(72) 発明者 モラン、タル  
イスラエル国 テル アビブ、ホフェイン ストリート 10  
(74) 代理人 弁理士 浅村 皓 (外3名)

最終頁に続く

(54) 【発明の名称】 アプリケーションのプロトコル特性を抽出するための方法とシステム

(57) 【要約】

任意のアプリケーションに対して自動的に、かつ継続的にアプリケーションプロトコルを抽出する(すなわち、許容可能、即ち認められた処置の組を限定する)ための方法とコンピュータプログラム。この方法では、サーバ(10)からのメッセージを、それが送られる前またはクライアント(12)へ送るとの並行して、受信する。このメッセージはクライアント(12)からのそれに対する特定の要求に応じたものであってもよい。次に、プログラムはサーバ(10)のメッセージからアプリケーションプロトコルデータを抽出する。メッセージのコピーに作用して、プログラムはメッセージから通信プロトコル(一つまたは複数)を取り去り、残りのメッセージを解析することにより、コマンド、フィールド等のようなメッセージに含まれる、ユーザが選択することができるオプションを識別する。これらのアイテムは、メッセージに述べられたようなアプリケーションの現在のバージョンの特定の段階に対する許容可能、即ち認められたユーザの処置の組を表す。次に、許容可能なユーザの処置の組は抽出プログラムによって、ゲートウェイまたは



**【特許請求の範囲】**

【請求項1】 サーバに存在するアプリケーションプログラムに対する1組の許容可能な処置を限定するための方法であって、

一つ以上のクライアント宛てにサーバが送信するメッセージを受信し、

前記サーバメッセージからアプリケーションプロトコルデータを抽出することにより、前記サーバメッセージに応答して取られ得る許容可能な処置の組を検索し、

抽出された前記アプリケーションプロトコルデータをプロトコルデータベースに記憶する、ことを備えた方法。

【請求項2】 請求項1の方法であって、アプリケーションプロトコルデータを抽出する前記ステップが、メッセージから通信プロトコルデータを取り去ることを含む、方法。

【請求項3】 請求項2の方法であって、アプリケーションプロトコルデータを抽出する前記ステップが、通信プロトコルデータを取り去った後にメッセージを解析することにより、メッセージに含まれるプロトコルを識別することを含む、方法。

【請求項4】 請求項2の方法であって、メッセージの宛て先のクライアントからの要求に응答してサーバメッセージが送られ、前記方法はクライアントのアドレスを表す前記取り去られた通信プロトコルデータまたはその一部を記憶することを含む、方法。

【請求項5】 請求項4の方法であって、抽出されたアプリケーションプロトコルデータをプロトコルデータベースに記憶する前記ステップが、クライアントアドレスを表す通信プロトコルデータに対応して、前記抽出されたアプリケーションプロトコルデータを記憶することにより、クライアントとのセッションを可能にすることを含む、方法。

【請求項6】 外部演算環境と内部演算環境との間に挿入されるセキュリティ・ゲートウェイ・システムであって、

前記内部演算環境に存在するアプリケーションプログラムに取り込まれ得る1組の許容可能な処置を記憶するプロトコルデータベースと、

前記外部演算環境から外部メッセージを受信し、前記プロトコルデータベースに問い合わせ、前記プロトコルデータベースに含まれていない前記外部メッセージのどの部分をも前記内部環境に送ることを拒絶するフィルタモジュールと、

前記内部演算環境から内部メッセージを受信し、アプリケーションプロトコルデータを前記内部メッセージから抽出し、抽出された前記アプリケーションプロトコルデータを前記プロトコルデータベースに記憶するプロトコル抽出モジュールと、

を備えたセキュリティ・ゲートウェイ・システム。

【請求項7】 請求項6のセキュリティ・ゲートウェイ・システムであって、前記フィルタモジュールが、外部環境から一つ以上の外部環境プロトコルで表される内容を含む外部メッセージを受信し、一つ以上の外部環境プロトコルで表されるメッセージに含まれ得る所定の内容に対してだけ簡略化された表現を定義する簡略化されたプロトコルに従って、前記外部メッセージの全部または一部を内容の簡略化された表現に写像することにより、前記外部メッセージを簡略化されたメッセージに変換し、前記簡略化されたメッセージを送信する第一の処理エンティティを含む、セキュリティ・ゲートウェイ・システム。

【請求項8】 請求項7のシステムであって、

前記第一の処理エンティティによって送信される前記簡略化されたメッセージを受信し、一つ以上の内部環境プロトコルに従って内容の簡略化された表現を内容の内部表現に写像することにより、簡略化されたメッセージを内部メッセージに変換し、該内部メッセージを前記内部演算環境で動作するアプリケーションに送信する第二の処理エンティティと、

前記簡略化されたメッセージを転送する前記第一の処理エンティティと前記第二の処理エンティティとの間の通信チャネルとを含むシステム。

【請求項9】 請求項8のシステムであって、前記プロトコル抽出モジュールが前記第二の処理エンティティの中に含まれている、システム。

【請求項10】 サーバをクライアントに接続することができる通信システムで、サーバに存在する一つ以上のアプリケーションプログラムに対して許容可

能な処置にクライアントを限定する方法であって、

一つ以上のクライアント宛てにサーバが送信するメッセージを受信し、

前記サーバメッセージから、前記サーバメッセージの各々に応答して取られ得る許容可能な処置のサーバメッセージ組を得て、

各々の要求がクライアントが要求する一つ以上の処置を含む、サーバ宛ての要求をクライアントから受信し、

前記要求の各々の中の前記一つ以上の処置を、許容可能な処置の前記組の少なくとも一つの組と比較し、

許容可能な処置の前記少なくとも一つの組の中にない要求に含まれるどの処置も許容しないこと、

を備えた方法。

## 【発明の詳細な説明】

## 【0001】

## (発明の背景)

本発明は一般にネットワークのセキュリティとプライバシーのシステムに関するものであり、更に詳しくはサーバで動作するアプリケーションプログラムで取ることができる処置を継続的に、そして自動的または半自動的に限定し、更新するための方法とシステムに関するものである。

## 【0002】

サーバコンピュータにあるデータまたはアプリケーションプログラムのセキュリティまたはプライバシーを危うくする一つの様式は、認められていないコマンドによるものである。すなわち、たとえばインターネットを介してサーバに接続できるクライアントコンピュータは、クライアントが資格を与えられていないデータの検索または命令の実行のための要求を送信することがある。たとえば、販売されている商品を手に入れるインターネットでアクセスできるウェブサーバは、購入品目の選択、個人および支払いのデータの入力、更には、前に入力されたデータを検索するためのアプリケーションプログラムの実行、のような処置を許容することがある。しかし、ウェブサーバはあるクライアントが価格データを変更したり、秘密にしておくつもりの他のデータを検索することを許容するべきではなく、また、これらの型の要求はそのクライアントに対して認められていない、または許容されていないと考えるべきである。現在、多くのアプリケーションは、クライアントがこれらの種類の要求を行うのに対する防御手段を含んでいない。

## 【0003】

現在、サービスプロバイダネットワーク（たとえば、商業サイト、政府の研究所、eコマースサイト等）はファイアウォール・セキュリティ装置またはルータによって防護されることが多い。これらのツールは、低レベルプロトコル（たとえば、TCPまたはUDP）の、そしてFTPまたはTELNETのような一般的なインターネットアプリケーションの弱点に基づいて、攻撃に対する良好なレベルのセキュリティを与える。しかし、これらのプロトコルは、特定のバンキン

アプリケーション、料金請求アプリケーション、保険アプリケーション等のような特定のアプリケーションプロトコルの実行を防ぐことができず、またアプリケーションプロトコルの変更または更新に責任を持つことができない。

#### 【0004】

クライアントが許容不可能な処置を取らないようにするために、クライアントとサーバとの間にゲートウェイまたはフィルタの機構を設けて、許容されていない要求を識別して、除去することがある。図1に示すように、フィルタモジュール14がサーバ10とクライアントとの間に配置される。クライアントは、図1では一つだけがクライアント12として示されている。フィルタモジュール14はクライアント12から要求を受け、クライアント12がサーバ10に要求する許容不可能な処置を除去し、要求の残りの許容される部分をサーバ10に送る。フィルタモジュール14は、プロトコルデータベース16に問い合わせることによってどの要求が許容されるか判定する。プロトコルデータベース16はサーバにあるアプリケーションプログラムに対するアプリケーションプロトコルを記憶している。ここで使用されているように、アプリケーションプロトコルはアプリケーションプログラムに対して許容可能な処置の一部または全部を表す。

#### 【0005】

ゲートウェイシステムと関連の構成要素の一例は後記出願番号09/149, 911および09/150, 112に説明されている。これらの出願はここに引用することにより、本出願の一部として組み入れられる。

#### 【0006】

プロトコルデータベース16を作成するために、開発者はアプリケーションのすべてのプロトコル、および認められた、または許容可能な処置を知っていなければならない。しかし、複雑なプロトコルを利用するアプリケーションの場合、精密なプロトコルを指定するプロセスは長く、冗長なものとなり得る。更に、アプリケーション開発者はプロトコルの完全な仕様を知っていないことさえ多い。プログラマが行う暗黙の仮定は通常、識別するのが極めて難しいからである。更に、開発者はアプリケーションプロトコルの変化を監視して、それに応じてプロトコルデータベースを更新しなければならない。完全で正確なプロトコルデータ

ベースをそなえ損なうと、クライアントがサーバにあるアプリケーションプログラムを充分に利用することができなくなり得る。効果的でないデータベースでは、アプリケーションプログラムの現在のバージョンでは許容不可能な処置をクライアントが取り得ることになってしまう。

#### 【0007】

したがって、オンライン、実時間ベースでサーバにあるアプリケーションに対するアプリケーションプロトコルを少なくとも半自動的に限定するための方法とシステムが求められている。

#### 【0008】

##### (発明の概要)

本発明の一つの目的は、セキュリティとプライバシーのシステムで前記の問題を解決することである。

本発明のもう一つの目的は、クライアントがサーバに要求することがあり得る、許容可能な処置を限定することである。

本発明のもう一つの目的は、オンライン、実時間ベースでアプリケーションプロトコルを抽出するための機構を提供することである。

#### 【0009】

これらの目的および他の目的は、アプリケーションプロトコルを抽出し、それにより、一組の許容可能な、即ち認められた処置を限定する、抽出コンピュータプログラムによって実現される方法によって達成される。この方法では、サーバからのメッセージを、それが送られる前またはクライアントへ送ると並行して、受信する。このメッセージはクライアントからのそれに対する特定の要求に応じたものであってもよい。たとえば、クライアントが通常、ブラウザプログラムを介してウェブドキュメントまたはページを要求するワールドワイドウェブの場合には、要求されたウェブページが、クライアントへの送信の前またはそれと並行してさえぎられる。

#### 【0010】

次に、抽出プログラムはサーバメッセージからアプリケーションプロトコルデータを抽出する。サーバメッセージは通常、インターネット通信の場合のTCP

／IPのような、クライアントへの送信に必要な一つ以上の通信プロトコルのためのデータを含む。メッセージのコピーに作用して、プログラムはメッセージからの通信データを解析し、この情報の記憶または廃棄を行う。次に、プログラムはメッセージからプロトコル（一つまたは複数）を取り去る。次に、プログラムは残りのメッセージを解析することにより、コマンド、フィールド、またはメッセージに含まれるユーザが選択することができる他のオプションを識別する。これらのアイテムは、メッセージに述べられたようなアプリケーションに対する許容可能な、即ち認められたユーザの処置の組を表す。

#### 【0011】

次に、許容可能なユーザの処置の組は抽出プログラムによって、ゲートウェイまたはフィルタモジュールにアクセスすることができるプロトコルデータベースに記憶される。プロトコルデータはセッションベースでセッションに記憶してもよく、その場合、それをフィルタモジュールが使用することにより、各個別のクライアント／サーバのセッションに対する、かつアプリケーションプログラムの各部分またはセグメントに対するプロトコルポリシーを増強する。このように使用されたとき、プロトコルデータは、任意の与えられた点で許容される処置を表すように継続的に更新と変更を行ってもよい。代わりに、ある期間にわたって多数のセッションからプロトコルデータを集めて記憶することにより、より大きく、より複雑なプロトコルデータベースを作成してもよい。

#### 【0012】

いずれにしても、サーバメッセージからアプリケーションプロトコルを獲得することにより、進行している実時間ベースで継続的に更新することができ、許容可能な処置の組をより正確に反映するプロトコルデータベースが提供される。

#### 【0013】

（好適実施例の詳細な説明）

次に、図面を参照して本発明の好適実施例を詳細に説明する。

#### 【0014】

図2に示すように、インターネット、イントラネット、または他の任意の専用ネットワークのようなコンピュータネットワークがクライアント12とサーバ1



0を接続する。クライアントとサーバは各々一つずつしか示していない。サーバ10には、フィルタモジュール14、プロトコルデータベース16、およびプロトコル抽出モジュール18で構成されるセキュリティ・ゲートウェイ・システムが結合されている。これらのモジュールはサーバ10に記憶してもよいし、サーバ10とは分離しているが、サーバ10に接続可能な一つのコンピュータに記憶してもよいし、分離しているが、接続可能な多数のコンピュータに記憶してもよい。

#### 【0015】

フィルタモジュール14はクライアント12からの要求のようなメッセージをさえぎり、プロトコルデータベース16に問い合わせ、要求の中の処置またはコマンドがクライアント12に対して認められたか、または許容されたか判定する。プロトコルデータベース16は、与えられたクライアント／サーバのセッションに対して、アプリケーションプログラムの「ステージ」または部分に対して、または与えられたアプリケーションプログラムに対して許容可能な処置の静的なリストとして、許容可能な処置のリストを含む。

#### 【0016】

いくつかの実施例では、フィルタモジュール14は出願番号09/149,911に説明されているように二つ以上の構成要素で構成され、これらを介してクライアント通信のコマンドおよび他のデータが、セキュリティを付加するための、簡略化されたプロトコルに変換される。図2Aに示されるように、ゲートウェイ14aは、専用の安全な通信バス28を介して接続され、ここではロボットと呼ばれる二つの分離した異なる処理エンティティ24、26を含む。内部ロボット24はサーバ10に接続され、外部ロボット26はインターネットまたは他の外部演算環境を介してクライアント12に接続される。各ロボットは、ここでクリア・インタ・プロトコルすなわちCIP (clear inter-protocol) と呼ばれる簡略化されたプロトコルフォーマットを使用して、それぞれの環境から受信された通信またはメッセージを簡略化されたメッセージに翻訳またはリダクションし、インタ・ロボットバス28を使用し、ロボット間転送プロトコルすなわちIRP (inter-robot transfer pro

t o c o l) を使用してC I Pメッセージを他方のロボットに送信し、他方のロボットから受信されたこのようなC I Pメッセージをそれぞれの環境に対してフォーマット化されたメッセージに翻訳することができる。これらの3個の要素24、26、28は協同して、保護される内部サーバ10に対してゲートウェイ14aが与える保護を実行する。ロボット24、26は、それぞれのセキュリティ・ゲートウェイのソフトウェアパッケージによって限定されるルーチンを実行する二つの別個の独立した論理プロセスである。ロボット24、26は二つの別個の処理装置に設置してもよいし、保護モードでロボット24、26の一方または両方を動作させる単一の処理装置に設置してもよい。

#### 【0017】

各ロボット24、26はプロトコルマネジャ（図示しない）を含むか、またはプロトコルマネジャにアクセスする。プロトコルマネジャは特定の環境に対してロボットが受信したメッセージをC I Pメッセージにリダクションして、他方のロボットに送信し、またC I Pフォーマットで他方のロボットから受信したメッセージをそれぞれの自然環境に対するプロトコルに再翻訳もする。したがって、プロトコルマネジャは、このリダクションと再翻訳のためにC I Pコードのデータベースを使用する。図2Aに示されるように、内部ロボット24の中にあるプロトコル抽出モジュール18は、内部ロボット24がサーバ10から受信したメッセージの中のプロトコルを抽出し、ここに説明したようにプロトコルを抽出し、アプリケーションプロトコルデータをロボット26に与える。

#### 【0018】

本発明によれば、プロトコル抽出モジュール18はサーバのメッセージをさえぎり、プロトコルデータベース16に追加するためのアプリケーションプロトコルデータを抽出する。図3を参照して、一実施例による抽出モジュール18の動作を説明する。ステップ30で、サーバ10はクライアント宛てのメッセージを送信する。このメッセージは、サーバ10またはそれに接続されたコンピュータ上であってランするアプリケーションに関連する情報を含む。このメッセージはクライアントから前に受信された要求に対する応答であってもよい。ステップ32で、サーバのメッセージのコピーまたはメッセージ自体を使用して、アプリケ

ーションプロトコルデータがサーバメッセージから抽出される。後で更に詳しく説明するように、この抽出プロセスは多数の方法で行うことができ、これらの方法には、公知の手法を使用して、TCP/IPのような低レベルプロトコルすなわち通信プロトコルを識別し、IPソースデータのような所要のデータを保持しつつ、このようなプロトコルを取り去り、許容されるコマンドまたは認められた他のユーザの処置があるかメッセージの残りを探索することが含まれる。

#### 【0019】

抽出されると、ステップ34でアプリケーションプロトコルデータがプロトコルデータベース16に記憶される。プロトコルデータは、アプリケーションの現在のバージョンに関連する永久ファイルに追加してもよいし、特定のクライアント/サーバのセッションに対してだけ使用される一時的なセッションベースのファイルに追加してもよいし、特定のサーバメッセージに対してだけ使用された後に上書きされる一時ファイルに追加してもよい。これらのオプションのすべては、アプリケーションの変更に対する自動的な適応を考慮に入れ、また、アプリケーションの異なる部分または段階で許容可能な処置に対して責任をとるためプロトコルデータベースの継続的修正を考慮に入れている。これらのオプションの相違は、前のメッセージからのプロトコルが将来のメッセージに対して適切なままである程度のものである。

#### 【0020】

ステップ36で、サーバメッセージがクライアントに送信される。次にステップ38で、クライアントはサーバ宛ての要求を送信する。クライアントの要求は、サーバメッセージに対する正当な応答であるかも知れないし、あるいはアプリケーションに認められていないコマンドを実行させようとする試みであるかも知れない。ステップ40で、フィルタモジュール14はクライアントの要求をさえぎり、それを読み取って、プロトコルデータベースに問い合わせる。所望のセキュリティとプライバシーに応じて、問い合わせは、クライアント、サーバ、特定のアプリケーション、特定のセッション等を識別する必要があるかも知れない。

#### 【0021】

ステップ42で、要求はアプリケーションプロトコルデータベースと比較され

て、その要求が許容されるか否か判定される。ステップ44で、要求が許容される場合には、フィルタモジュール14は要求をサーバに送る。要求がプロトコルデータベース16内のアプリケーションプロトコルの処置のどれとも合致せず、したがって許容不可能と考えられる場合には、ステップ46で、要求はサーバへのアクセスを拒絶され、クライアント12とサーバ10の一方または両方に認められていない要求が試みられたことを通知することができる。

#### 【0022】

ウェブに基づく通信のために使用されるプロトコル抽出方法の一実施例が図5に示されている。ステップ60で、抽出モジュールはウェブドキュメントまたはHTMLページであるサーバメッセージを受信する。ステップ62で、TCP/IPプロトコルデータがドキュメントから抽出され、記憶されることにより、ソースIPアドレスの識別が助けられ、たとえば、メッセージの宛て先のクライアントとのセッションが維持される。ステップ64で、モジュールがHTMLデータを読み取るまで、HTTPのような他の通信データが更にドキュメントから取り去られる。

#### 【0023】

このデータから、モジュールは特定のアプリケーションの設計についての情報を集める。これは、ステップ66でHTMLドキュメントデータを解析し、すべてのタグを突き止めることにより行われる。ステップ68で他のウェブドキュメントへのリンクを定義するアンカーのようなタグの場合、ステップ70でURLとのリンクがプロトコルデータベースに追加される。これはたとえば、サーバ上の他の多くのページへのリンクを含むウェブサーバのホームページに当てはまる、またはShockwave、RealAudio、またはRealVideoのファイルに含まれるような、ある型のマルチメディアの中に埋め込まれたリンクに当てはまる。ステップ72で、抽出モジュールはウェブドキュメントの中の任意の入力フィールドも突き止める。これはたとえば、HTMLフォームの中に配置されているかも知れない。次に、ステップ74で、フィールドの型と長さを含む、このようなフィールドに対するフィールドデータのアイデンティティと性質がプロトコルデータベースに追加される。フィールド長が指定されない場合に

は、デフォルトフィールド長が使用される。たとえば、クライアント要求の与えられた長さの英数字データを必要とするものとして「ネーム」フィールドがプロトコルデータベースにリストされ、データフォーマット化された英数字データを必要とするものとして日付フィールドがリストされ、「メールアドレス」フィールドはメールアドレスフォーマット化されたデータ、たとえば、a@b.cを必要とする。

#### 【0024】

同様のステップを使用して、プロトコル抽出モジュールは、フォーム、フィールド、固定フィールド、隠れフィールド、メニューオプション、DOMコンポーネント等の検査も行う。これらの要素の各々に対して、プロトコルデータベースはそれらの性質およびそれに課される制約について更新される。たとえば、識別されたすべての隠れフィールドに対して、データベースはそれらの性質およびクライアントはそれらの内容を変更することはできないということについて更新される。

#### 【0025】

ステップ76で、抽出モジュールは更に、ウェブドキュメント内の利用できる他の任意の処置を識別する。これらは、たとえば、HTMLフォームの「サブミット」コマンド、「サーチ」コマンド、または他のアプリケーションレベルのプロトコルを含む。ステップ78で、ウェブドキュメント内のこれらの付加的な処置も抽出されて、プロトコルデータベースに記憶される。

#### 【0026】

ステップ80でゲートウェイまたはフィルタがクライアントの要求を受けると、ステップ82で、それは要求内の各リンク、データ、コマンド、または他の処置をプロトコルデータベースに現在記憶されている対応するエンティティと比較する。このような許容不可能な処置が要求の中にない場合には、ステップ84で、その要求はサーバに送信される。許容不可能な処置が要求の中にある場合には、ステップ86で、プロトコルデータベースの中に含まれていないリンク、データ、またはコマンドが要求から抹消されるか、またはその代わりに、要求全体が拒絶される。

## 【0027】

次に、図5および6に示すように、いくつかの実施例では、プロトコル抽出モジュールは抽出プロセスを統制的に働かせ、管理するプロトコル・ディスパッチャ100を含む。図5に示されるように、ディスパッチャ100は一度に一つのプロトコル90を抽出し、たとえば、TCP/IP、HTTP、HTML、および他の任意のプロトコルを開始する。ウェブ環境では、メッセージを受信すると、図6のステップ110でディスパッチャ100は変数`current_protocol`をTCP/IPに初期設定する。次に、ステップ112で、現在のプロトコルからデータが抽出され、次に、ステップ114でメッセージから現在のプロトコルが取り去られる。次に、ステップ116で、現在のプロトコルがプロトコルデータベースに記憶されるか、またはその代わりに、ディスパッチャ100がすべてのプロトコルを通して進んだ後、プロトコルデータベースを更新してもよい。

## 【0028】

次に、ステップ118で、変数`current_protocol`がインクリメントされるか、または新しいプロトコルに設定される。ステップ120で`current_protocol`がナル(NULL)で、抽出すべきプロトコルが無いことを示している場合には、プロセスは完了する。そうでなく、新しい現在のプロトコルに関連するデータがメッセージの中にある場合には、ステップ112でそのデータが抽出され、完了までプロセスが反復される。

## 【0029】

好適実施例に関連して本発明を説明し、図示してきたが、当業者には明らかなように本発明の趣旨と範囲から逸脱することなく多数の変更と変形を加えることができる。このような変更と変形は発明の範囲内に含まれるように意図されているので、本発明は前記の方法または構成の詳細に限定されるべきではない。

## 【0030】

## (著作権の告知)

この特許文書の開示の一部分は著作権保護を受ける資料を含む。著作権者は、特許登録商標庁の特許ファイルまたはレコードに現れたときに特許文書または特

許の開示を誰がファクシミリ複写しても異議を申し立てないが、それ以外の場合には、何であれ、すべての著作権を保留する。

【0031】

(関連出願)

この出願は、1998年9月9日に出願された出願番号09/149,911、「委託された内部ネットワークの動作を保護するための方法とシステム」(METHOD AND SYSTEM FOR PROTECTING OPERATIONS OF TRUSTED INTERNAL NETWORKS)、および1998年9月9日に出願された出願番号09/150,112、「アプリケーションプログラムまたはオペレーティングシステムに対して限定された動作環境を維持するための方法とシステム」(METHOD AND SYSTEM FOR MAINTAINING RESTRICTED OPERATING ENVIRONMENTS FOR APPLICATION PROGRAMS OR OPERATING SYSTEMS)に関連している。これらの関連出願はここに引用することにより、この明細書の一部として組み入れられる。

【図面の簡単な説明】

【図1】

クライアントの要求をフィルタリングするためのゲートウェイをそなえたクライアントサーバシステムのブロック図である。

【図2】

本発明に従って図1のシステムにプロトコル抽出モジュールを追加して得られたシステムのブロック図である。

【図2A】

ゲートウェイが外部ロボットおよび内部ロボットを含む、図2のシステムの一実施例のブロック図である。

【図3】

本発明によりオンラインベースでアプリケーションプロトコル内の許容可能な処置を限定するプロセスを示すフローチャートである。

## 【図4】

本発明の一実施例によりインターネットを介してウェブサーバから送信されるHTMLファイル内の許容可能な処置を限定するプロセスの一部を示すフローチャートである。

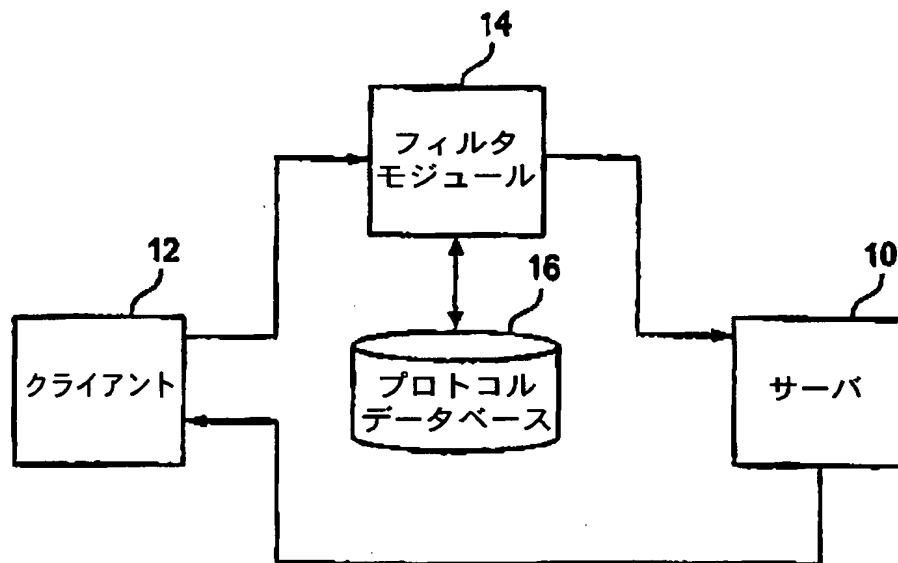
## 【図5】

本発明の一実施例によりHTMLファイルに作用する図2のプロトコル抽出モジュールのプロトコルディスパッチャ構成要素を示すブロック図である。

## 【図6】

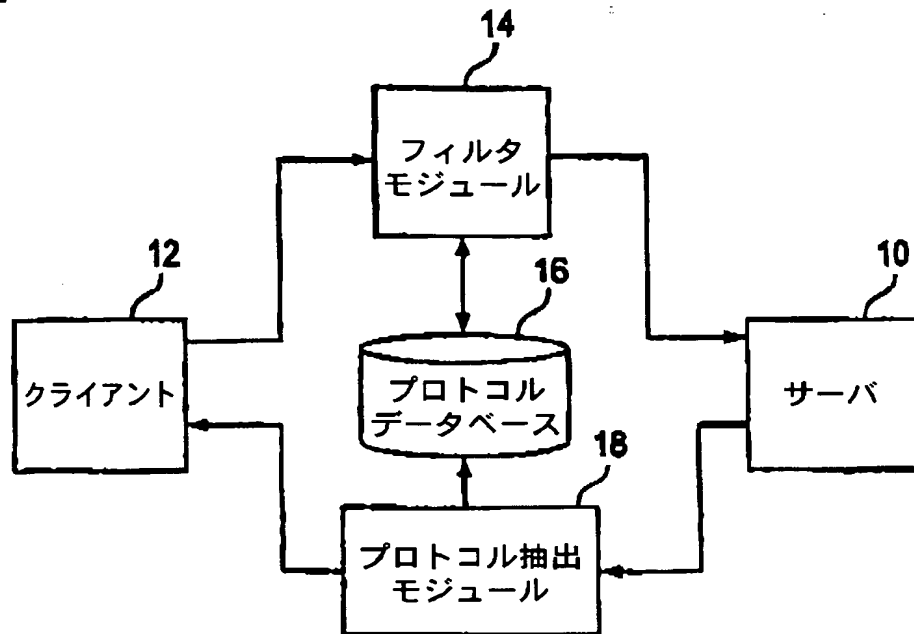
図5のプロトコルディスパッチャ構成要素により遂行されるプロトコル抽出プロセスを示すフローチャートである。

## 【図1】

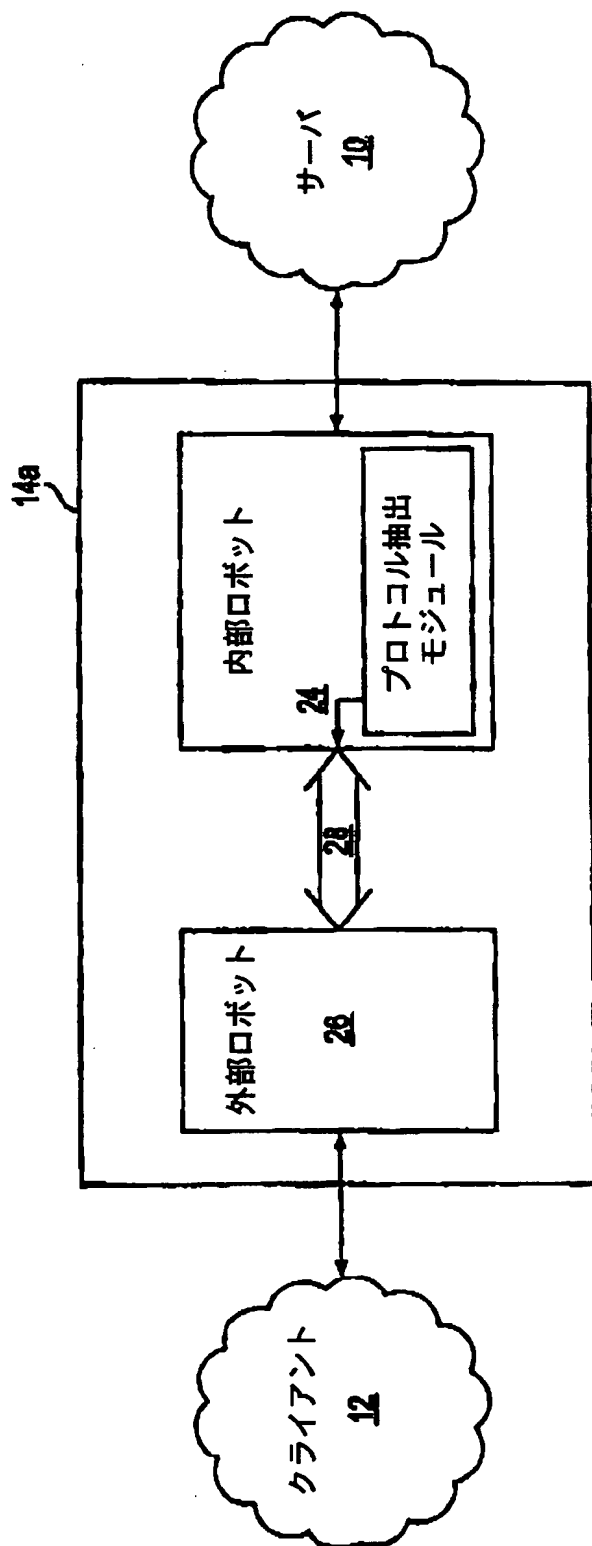




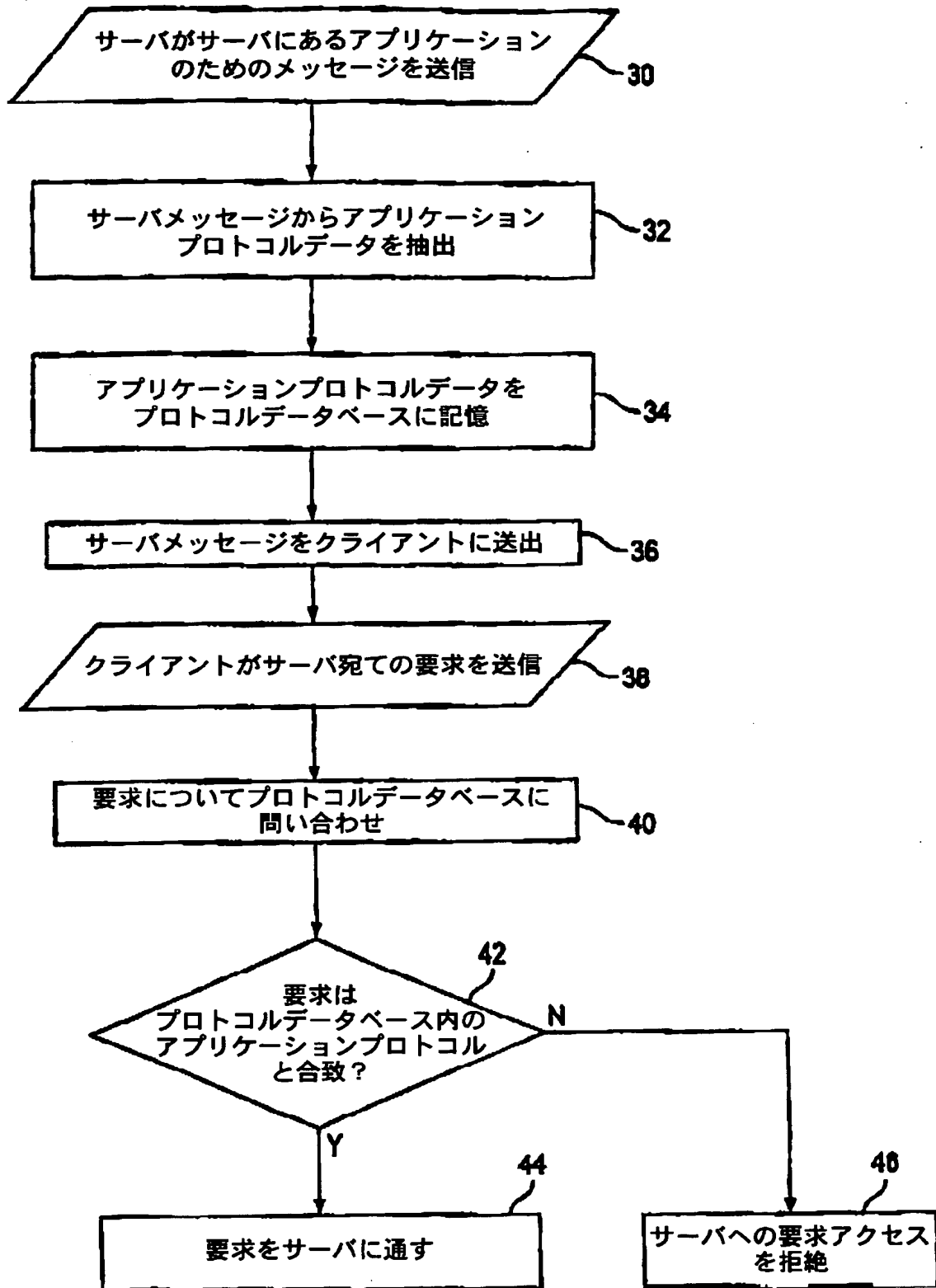
【図2】



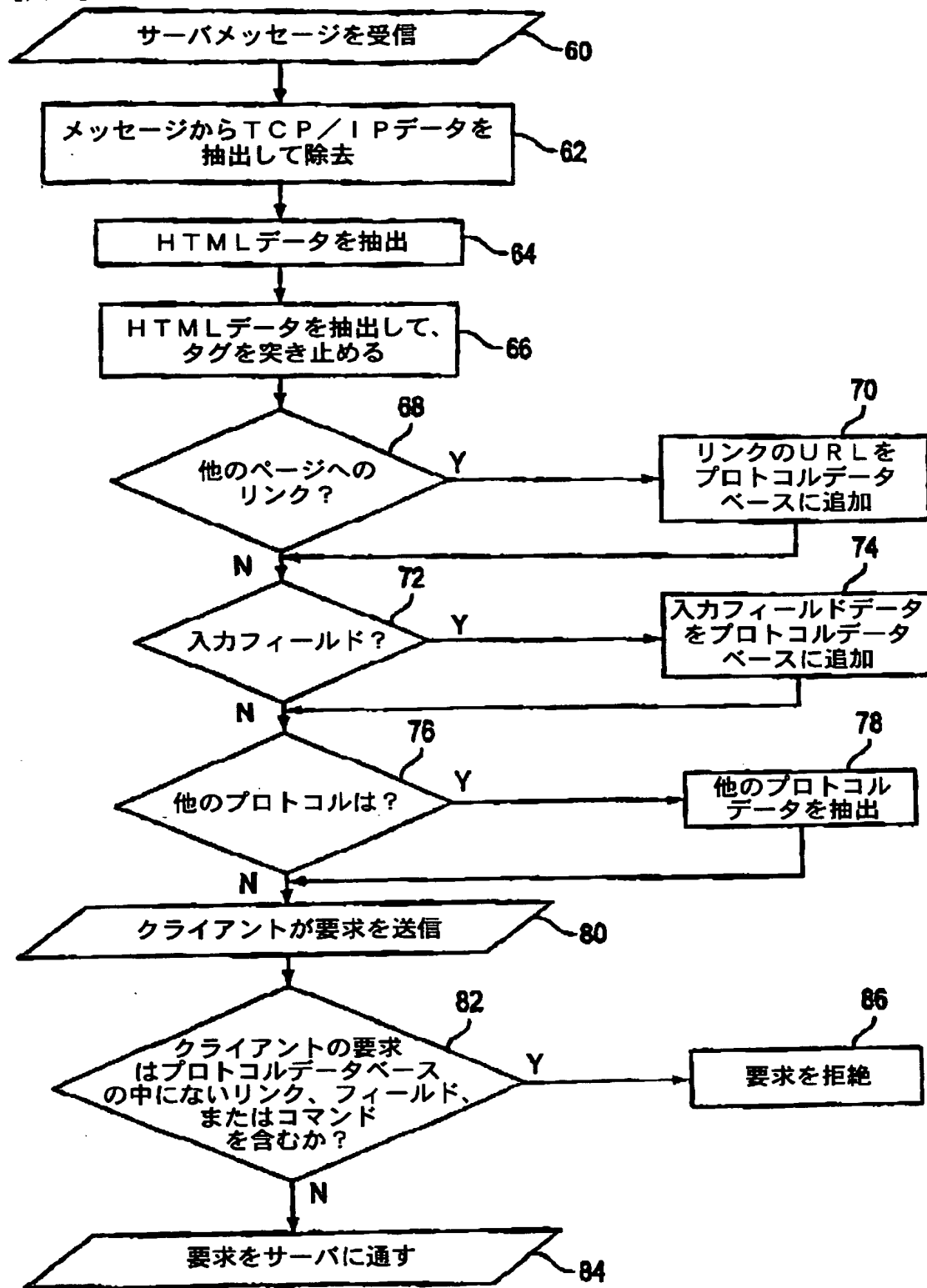
【図2A】



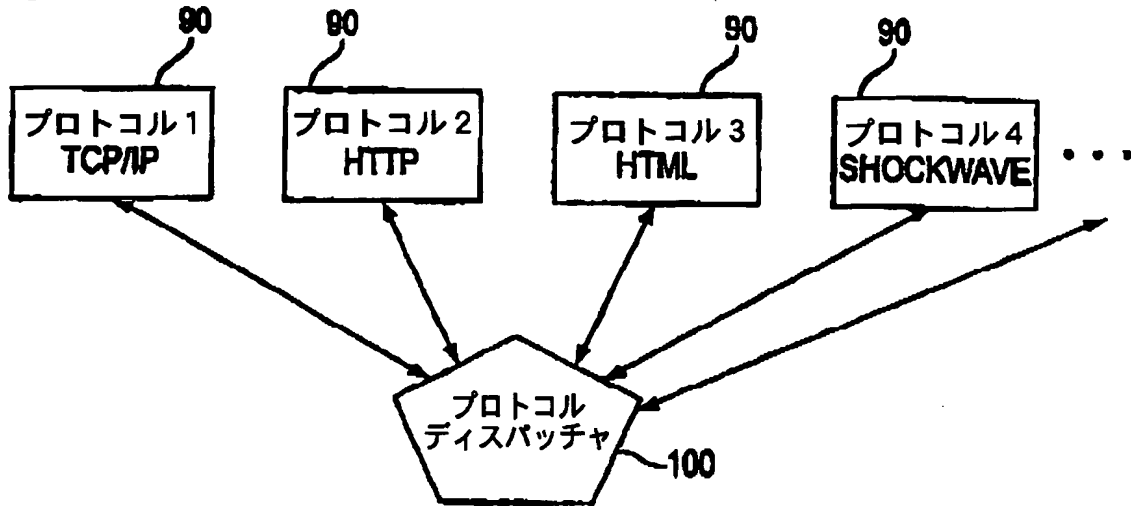
【図3】



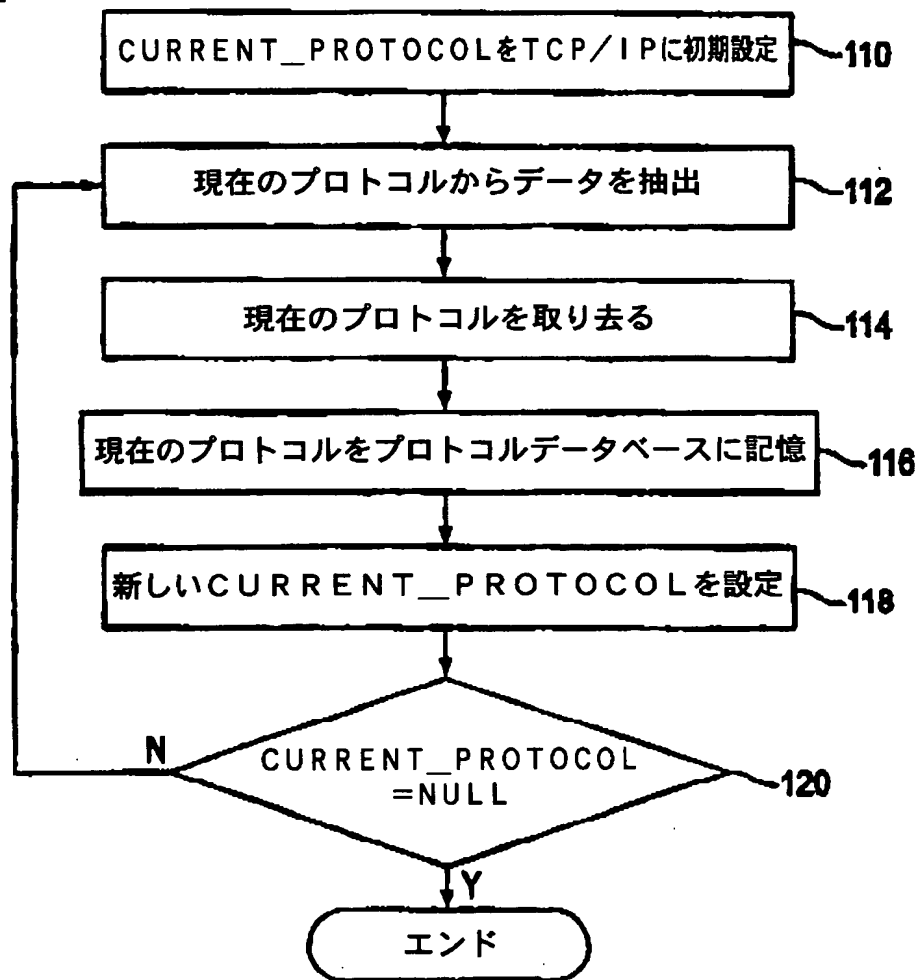
【図4】



【図5】



【図6】



## 【手続補正書】

【提出日】平成14年2月14日(2002. 2. 14)

## 【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】0014

【補正方法】変更

【補正の内容】

## 【0014】

図2Aに示すように、インターネット、イントラネット、または他の任意の専用ネットワークのようなコンピュータネットワークがクライアント12とサーバ10を接続する。クライアントとサーバは各々一つずつしか示していない。サーバ10には、フィルタモジュール14、プロトコルデータベース16、およびプロトコル抽出モジュール18で構成されるセキュリティ・ゲートウェイ・システムが結合されている。これらのモジュールはサーバ10に記憶してもよいし、サーバ10とは分離しているが、サーバ10に接続可能な一つのコンピュータに記憶してもよいし、分離しているが、接続可能な多数のコンピュータに記憶してもよい。

## 【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】0016

【補正方法】変更

【補正の内容】

## 【0016】

いくつかの実施例では、フィルタモジュール14は出願番号09/149,911に説明されているように二つ以上の構成要素で構成され、これらを介してクライアント通信のコマンドおよび他のデータが、セキュリティを付加するための、簡略化されたプロトコルに変換される。図2Bに示されるように、ゲートウェイ14aは、専用の安全な通信バス28を介して接続され、ここではロボットと呼ばれる二つの分離した異なる処理エンティティ24、26を含む。内部ロボッ

ト24はサーバ10に接続され、外部ロボット26はインターネットまたは他の外部演算環境を介してクライアント12に接続される。各ロボットは、ここでクリア・インタ・プロトコルすなわちCIP (clear inter-protocol) と呼ばれる簡略化されたプロトコルフォーマットを使用して、それぞれの環境から受信された通信またはメッセージを簡略化されたメッセージに翻訳またはリダクションし、インタ・ロボットバス28を使用し、ロボット間転送プロトコルすなわちIRP (inter-robot transfer protocol) を使用してCIPメッセージを他方のロボットに送信し、他方のロボットから受信されたこのようなCIPメッセージをそれぞれの環境に対してフォーマット化されたメッセージに翻訳することができる。これらの3つの要素24、26、28は協同して、保護される内部サーバ10に対してゲートウェイ14aが与える保護を実行する。ロボット24、26は、それぞれのセキュリティ・ゲートウェイのソフトウェアパッケージによって限定されるルーチンを実行する二つの別個の独立した論理プロセスである。ロボット24、26は二つの別個の処理装置に設置してもよいし、保護モードでロボット24、26の一方または両方を動作させる単一の処理装置に設置してもよい。

【手続補正3】

【補正対象書類名】明細書

【補正対象項目名】0017

【補正方法】変更

【補正の内容】

【0017】

各ロボット24、26はプロトコルマネージャ（図示しない）を含むか、またはプロトコルマネージャにアクセスする。プロトコルマネージャは特定の環境に対してロボットが受信したメッセージをCIPメッセージにリダクションして、他方のロボットに送信し、またCIPフォーマットで他方のロボットから受信したメッセージをそれぞれの自然環境に対するプロトコルに再翻訳もする。したがって、プロトコルマネージャは、このリダクションと再翻訳のためにCIPコードのデータベースを使用する。図2Bに示されるように、内部ロボット24の中にあるプ

ロトコル抽出モジュール18は、内部ロボット24がサーバ10から受信したメッセージの中のプロトコルを抽出し、ここに説明したようにプロトコルを抽出し、アプリケーションプロトコルデータをロボット26に与える。

【手続補正4】

【補正対象書類名】明細書

【補正対象項目名】図面の簡単な説明

【補正方法】変更

【補正の内容】

【図面の簡単な説明】

【図1】

クライアントの要求をフィルタリングするためのゲートウェイをそなえたクライアントサーバシステムのブロック図である。

【図2A】

本発明に従って図1のシステムにプロトコル抽出モジュールを追加して得られたシステムのブロック図である。

【図2B】

ゲートウェイが外部ロボットおよび内部ロボットを含む、図2Aのシステムの一実施例のブロック図である。

【図3】

本発明によりオンラインベースでアプリケーションプロトコル内の許容可能な処置を限定するプロセスを示すフローチャートである。

【図4】

本発明の一実施例によりインターネットを介してウェブサーバから送信されるHTMLファイル内の許容可能な処置を限定するプロセスの一部を示すフローチャートである。

【図5】

本発明の一実施例によりHTMLファイルに作用する図2Aのプロトコル抽出モジュールのプロトコルディスパッチャ構成要素を示すブロック図である。

【図6】



図5のプロトコルディスパッチャ構成要素により遂行されるプロトコル抽出プロセスを示すフローチャートである。

【手続補正5】

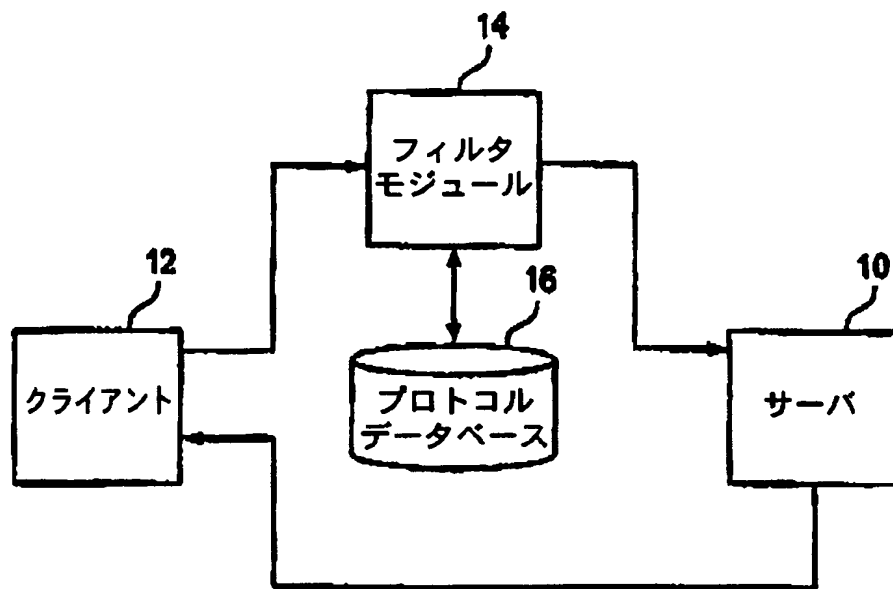
【補正対象書類名】図面

【補正対象項目名】全図

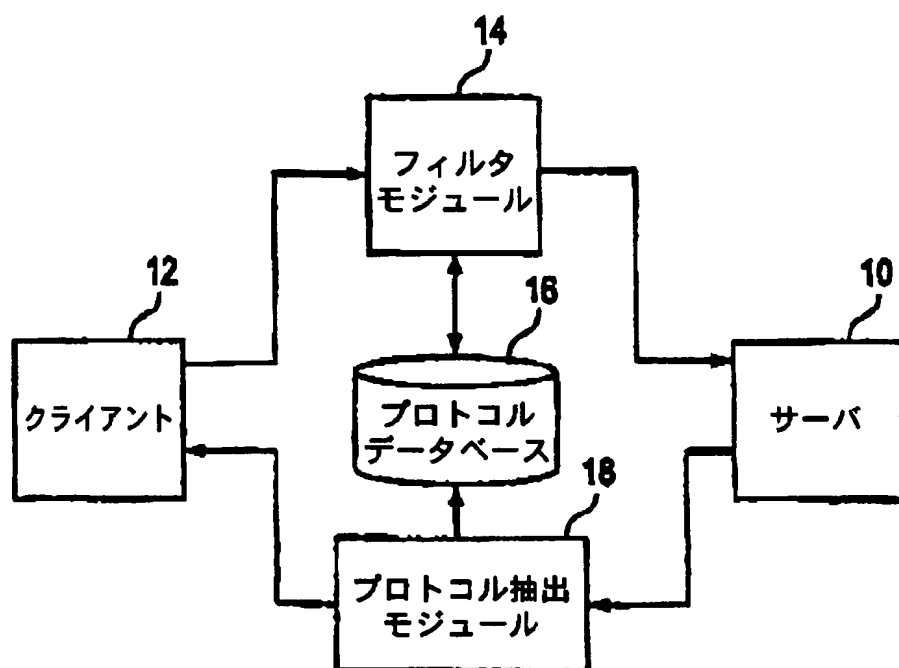
【補正方法】変更

【補正の内容】

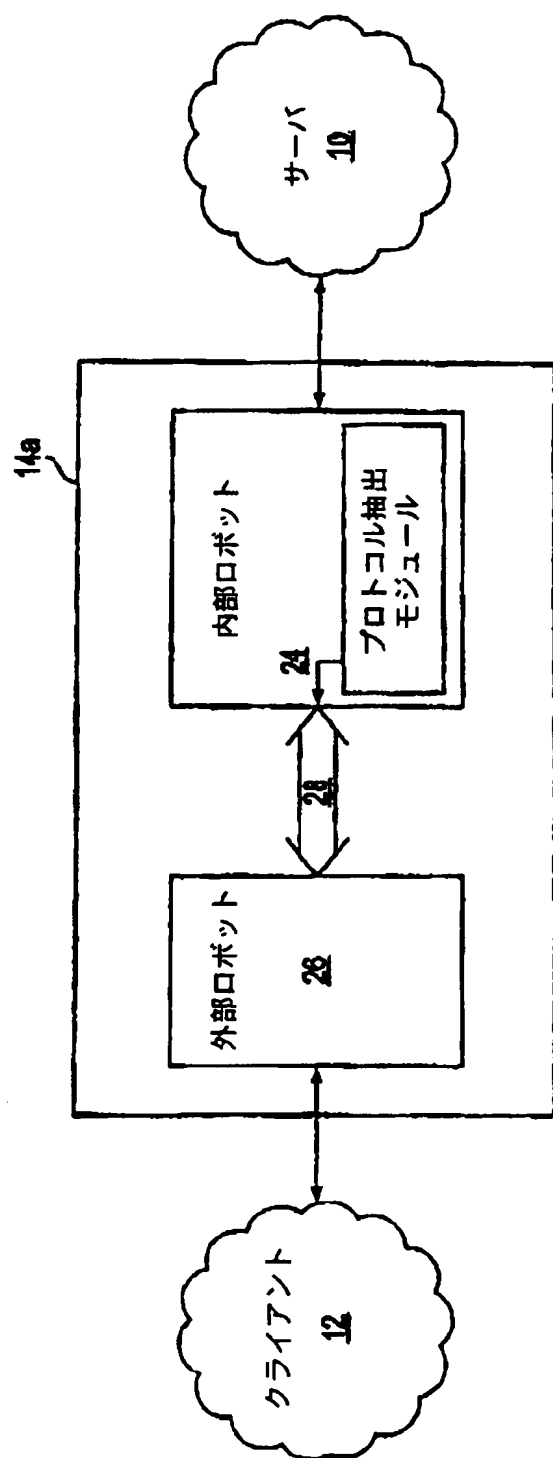
【図1】



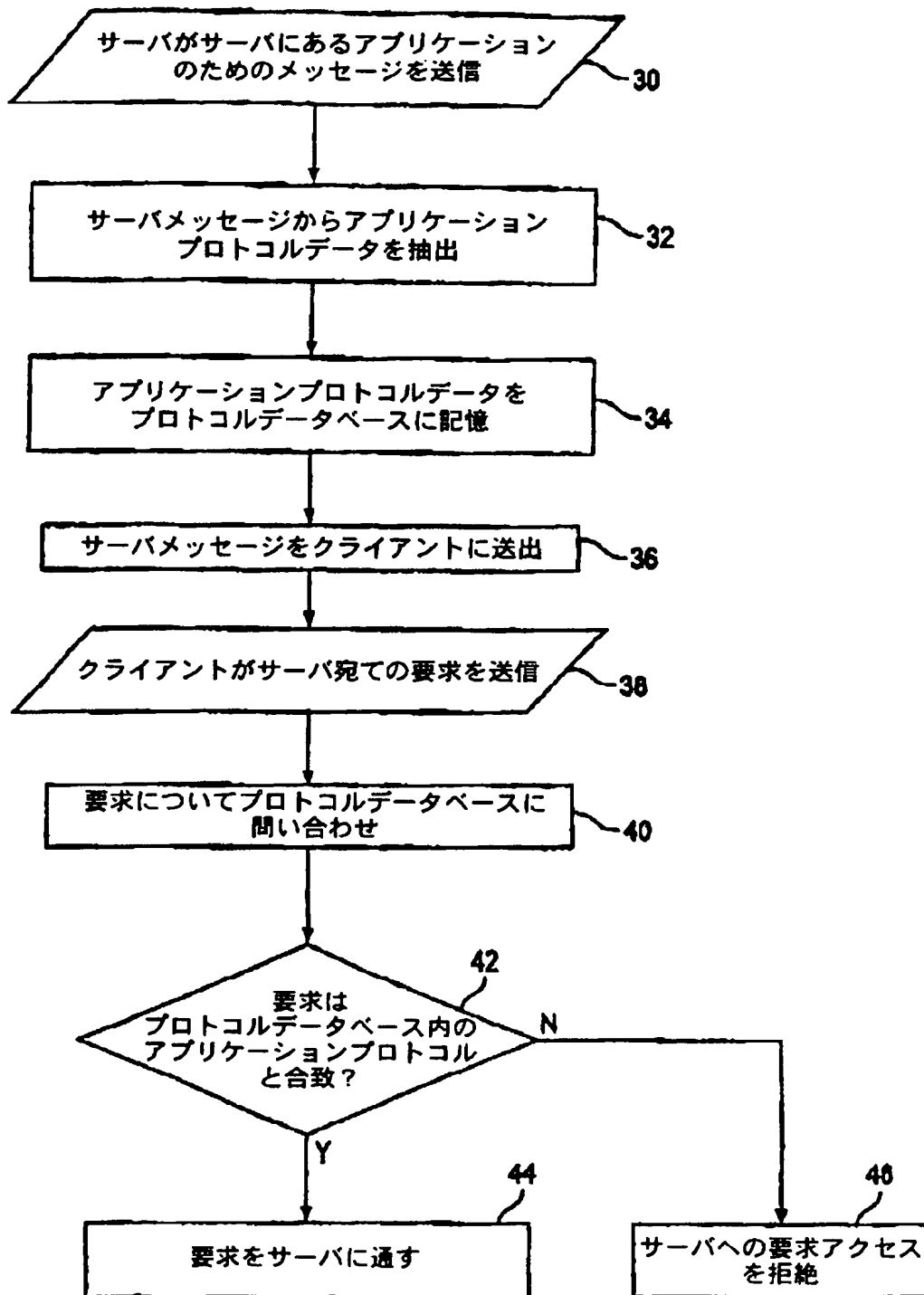
【図2A】



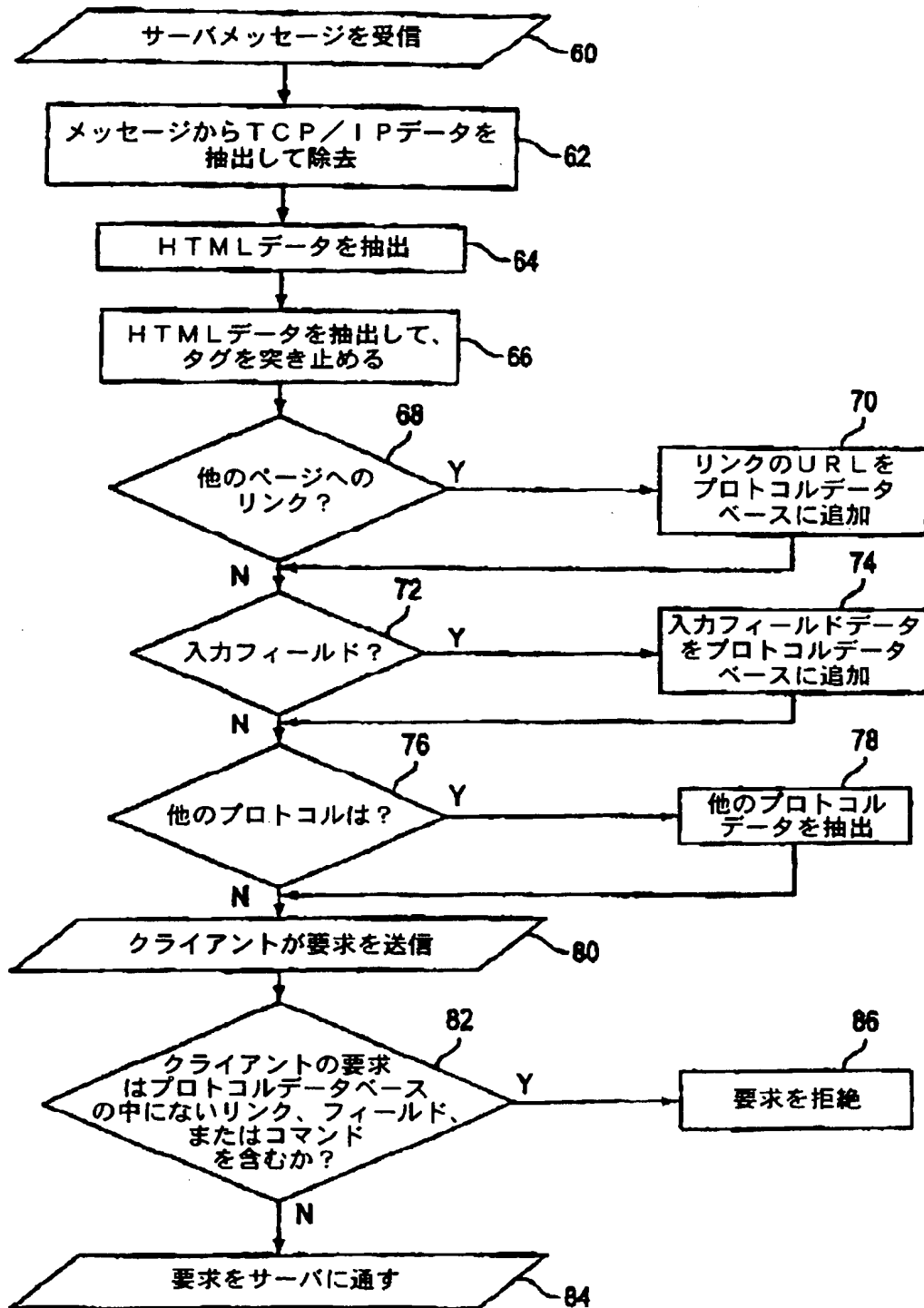
【図2B】



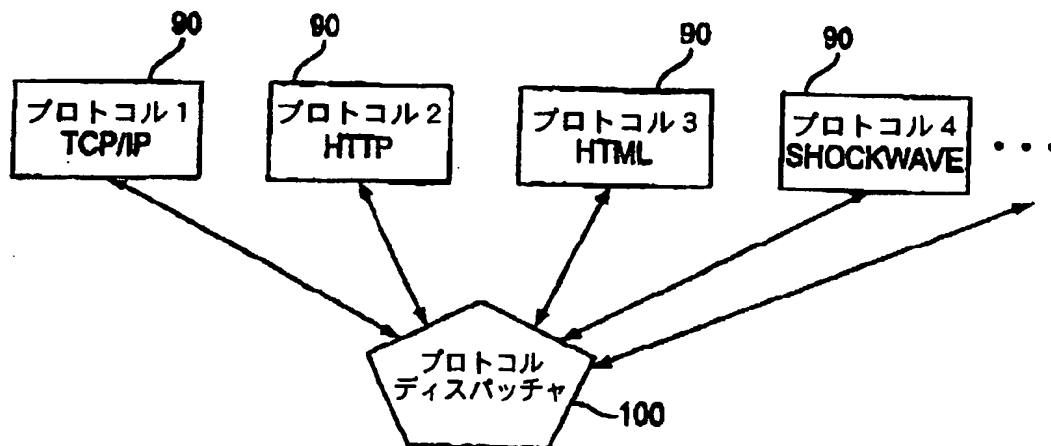
【図3】



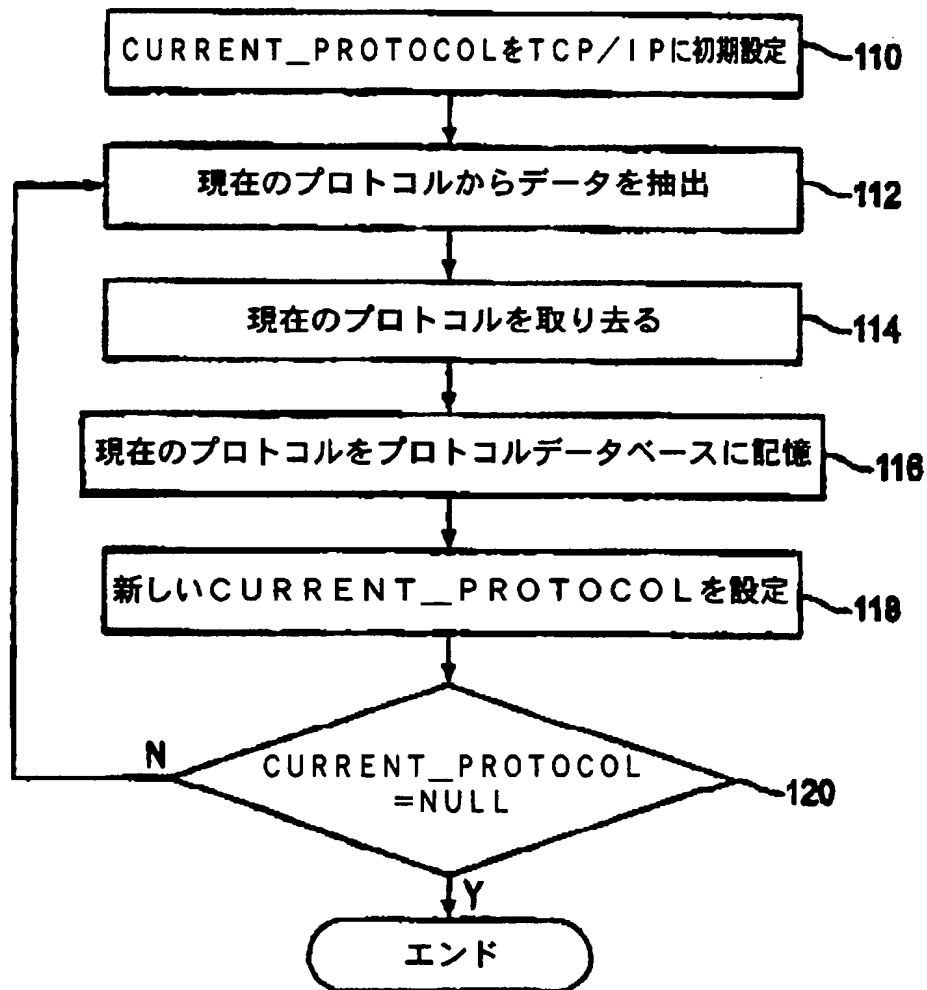
【図4】



【図5】



【図6】



## 【国際調査報告】

## INTERNATIONAL SEARCH REPORT

International application No.  
PCT/IL00/00378

<b>A. CLASSIFICATION OF SUBJECT MATTER</b> IPC(7) : 006F 13/00; H04L 12/66 US CL : Please See Extra Sheet According to International Patent Classification (IPC) or to both national classification and IPC		
<b>B. FIELDS SEARCHED</b> Minimum documentation searched (classification system followed by classification symbols) U.S. : 713/200, 201, 202, 151, 152, 153; 709/223, 224, 225, 226, 227, 230 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched NONE Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) NONE		
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,778,189 A (KIMURA et al.) 07 July 1998, abstract, col 1, lines 24-67, col 2, lines 1-67, col 3, lines 9-25, col 4, lines 27-67.	1-10
X	US 5,724,355 A (BRUNO et al.) 03 March 1998, abstract, col 1, lines 13-67, col 2, lines 1-49, col 3, lines 1-24, col 4, lines 1-28.	1-10
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
* Special categories of cited documents:		
*A* document defining the general state of the art which is not considered to be of particular relevance		*T* later document published after the international filing date or priority date and not in conflict with the application but used to understand the principle or theory underlying the invention
*B* earlier document published on or after the international filing date		*X* document of particular relevance, the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
*L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)		*Y* document of particular relevance, the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
*O* document referring to an oral disclosure, use, exhibition or other means		*Z* document member of the same patent family
*P* document published prior to the international filing date but later than the priority date claimed		
Date of the actual completion of the international search 01 SEPTEMBER 2000		Date of mailing of the international search report 03 OCT 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230		Authorized officer BEAUSOLEIL ROBERT Telephone No. (703) 305-4987 <i>R. Yegorov</i>

Form PCT/ISA/210 (second sheet) (July 1998)\*

## INTERNATIONAL SEARCH REPORT

International application No.  
PCT/IL00/00378

A. CLASSIFICATION OF SUBJECT MATTER:  
US CL :

713/200, 201, 202, 151, 152, 153; 709/223, 224, 225, 226, 227, 230



## フロントページの続き

(81) 指定国 EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW

(72) 発明者 ギャラント、ヤロン

アメリカ合衆国 カリフォルニア、マウンテンビュー、サウス レングストーフ アヴェニュー 575、アパートメント 51

(72) 発明者 エル — ハナニ、ユーヴァル

イスラエル国 テル アビブ、イエシュラン ストリート 3

(72) 発明者 リシェフ、エラン

アメリカ合衆国 カリフォルニア、サニーヴェイル、オールド サン フランシスコ ロード 718

Fターム(参考) 5B089 GA11 GA31 JA35 KA17 KB13  
KC47 KC53 KC54 KF04 KH04  
MC08

## 【要約の続き】

フィルタモジュール(14)にアクセスすることができるプロトコルデータベースに記憶される。